(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 December 2001 (13.12.2001)

PCT

(10) International Publication Number
WO 01/95327 A2

(51) International Patent Classification[7]: G11B 20/00

(21) International Application Number: PCT/EP01/05195

(22) International Filing Date: 8 May 2001 (08.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
00201951.1 2 June 2000 (02.06.2000) EP

(71) Applicant: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors: **LINNARTZ, Johan, P., M., G.**; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **KALKER, Antonius, A., C., M.**; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **TALSTRA, Johan, C.**; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: **DEGUELLE, Wilhelmus, H., G.**; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

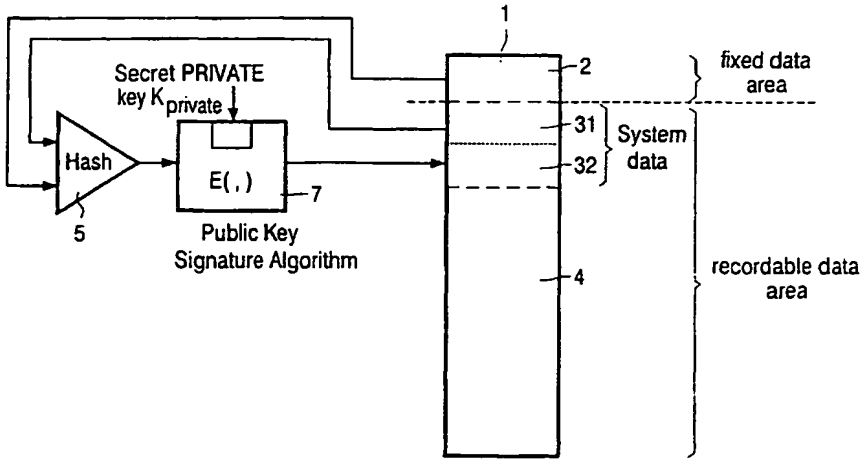
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: RECORDABLE STORAGE MEDIUM WITH PROTECTED DATA AREA



(57) Abstract: The invention relates to a method of storing data on a rewritable data storage medium, to a corresponding storage medium, to a corresponding recording apparatus and to a corresponding playback apparatus. Copy-protective measures require that on rewritable storage media some data must be stored which shall not be modifiable or erasable by consumer end products. A practical problem is the storage of large quantities of such data in a fixed data area. Typically the capacity is limited to a few bits. Meanwhile the amount of copy protection data that needs to be stored may well exceed the storage capacity available in the read-only fixed data area. The invention therefore proposes to write the copy protection data as system data in the recordable data area (4), e.g. as part of the formatting of the medium (1). A cryptographic summary is computed and also stored in the recordable data area (32) or in the fixed data area (2) such that a cryptographic relationship between the fixed data area (2) and the system data area (3) is provided. A playback or replay apparatus will only accept a storage medium with a valid combination of copy protection data and fixed data.

WO 01/95327 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Recordable storage medium with protected data area

The invention relates to a method of storing data on a rewritale data storage medium, to a storage medium, to a recording apparatus for storing data on a rewritable data storage medium and to a playback apparatus for playback of user data stored on a rewritable data storage medium.

The invention addresses a storage medium on which users can store copyrighted and copy-free material. Often the user has a right to store and copy content, but there are restrictions to the number of (generations of) copies that he can make. Encryption is used to ensure that copy-righted content can only be interpreted by "compliant" devices which adhere to copy protective restrictions. A further protection is needed to avoid that non-compliant devices can make a bitwise copy of encrypted data. This is often avoided by storing essential information, e.g. a decryption key, in a manner that can not be copied.

More generally it is concluded that copy-protective measures require that on recordable discs some data must be stored which shall not be modifiable or erasable by consumer end products. These data will be called "system data" in the following. Examples of "system data" are:

- a unique disc identifier number which is used to encrypt the data that the user stores on the disc,
- a list consisting of a single key which has been encrypted with a number of different manufacturer-specific or device-specific keys,
- a list of electronic serial numbers of revoked devices or revoked discs. By storing such a list on all blank discs, revocation instructions can be disseminated to consumer devices. Upon receipt of such revocation instructions, compliant devices refuse to communicate with revoked devices.

Content or data recorded by the user will be called "user data" in the following. Moreover, the term "fixed data area" will be used for an area of the storage medium in which any information is stored that is read-only and not modifiable by consumer devices. On the contrary, in the "recordable data area" information is stored which can be modified by consumer devices. Also data, which can only be written by consumer devices after some modifications ("hacks") have been made to the device by malicious users will be

stored in the recordable data area. Such modifications can be a change in the firmware or software used to control the recorder.

To store data in the fixed data area requires the use of components which are typically not available in consumer devices. An example of a technique to store such data is a "wobble", which is a radial deviation of the pit positions or the pregroove from a perfect spiral. Laws of physics and mechanics prohibit that such a wobble can be written on the fly by a laser as available in a consumer recorder for optical discs. Other examples of data stored in the fixed data area are the BCA code, proposed for DVD-ROM, selectively damaged spots on the disc material burned by high power lasers, or data stored in a special area of the disc which contains read-only material.

A practical problem is the storage of large quantities of data in the fixed data area. Typically the capacity is limited to a few (hundreds of) bits. Meanwhile the amount of system data that needs to be stored may well exceed the storage capacity available in the fixed data area.

The invention has therefore for its object to provide a method of storing data on a rewritable data storage medium according to which the above mentioned problems are overcome and which allows the storage of large quantities of system data in a tamper-resistant manner. Further, a corresponding storage medium, a corresponding recording apparatus and a corresponding playback apparatus shall be provided.

These objects are achieved according to the invention by a method as set forth in claim 1 or 2, by a storage medium as set forth in claim 9 or 10, by a recording apparatus as set forth in claim 12 or 13 and by a playback apparatus as set forth in claim 14 or 15.

The invention is mainly based on the idea that there exists some cryptographic relationship between data stored in the fixed data area and system data. This relationship is made up by the cryptographic summary which is according to the invention generated from the system data alone or from both the system data and identification data which can be a random number stored in the fixed data area. This cryptographic summary is used by a recording or playback apparatus to detect whether the system data have been tampered with, e.g. erased or modified in order to manipulate the copy proctection of the storage medium. The cryptographic summary is thus used for verification of the system data which means that in case of a verification failure playback or recording of the content of the storage medium can be stopped.

According to a first solution the system data are written in the recordable data area, e.g. as part of the formatting of the storage medium. A cryptographic summary, e.g. a

cryptographic hash, is computed over the system data, and the result of that cryptographic summary, e.g. the result of that hash, is stored in the fixed data area. A recording apparatus will then only accept a storage medium with a valid combination of system data and fixed data, i.e. cryptographic summary.

According to an alternative solution identification data, e.g. a random number, are created and stored in the fixed data area. The recordable data area then contains the user data, the system data and a cryptographic summary of the system data and the identification data, e.g. an electronic signature thereof. A recording or playback apparatus will then use a verifier (e.g. a public key) to check the validity of the cryptographic summary, the system data and the identification data, i.e. the validity of the signature will be checked. Instead of using an electronic signature a message authentication code (MAC) can be used for the verification which is cheaper but less secure.

Other preferred embodiments of the invention are disclosed in the dependent claims.

The invention and preferred embodiments thereof are explained hereinafter in more detail with reference to the following drawings in which

Fig. 1 shows a recording method according to a first embodiment,

Fig. 2 shows a playback method according to a first embodiment,

Fig. 3 shows a recording method according to a second embodiment,

Fig. 4 shows a playback method according to the second embodiment,

Fig. 5 shows a recording method according to a third embodiment and

Fig. 6 shows a playback method according to the third embodiment.

Figure 1 shows a diagram explaining the method of storing data on a rewritable data storage medium according to a first embodiment of the invention. The storage medium 1, which can be a disc for optical recording of data, e.g. at DVD or a CD, is separated into a read-only fixed data area 2 and a recordable data area 3, 4 which is subdivided into a system data area 3 and a user data area 4. Data stored in the fixed data area 2 can not be modified by consumers. A typical implementation of the fixed data area 2 is the pressing of pits into a rewritable disc, i.e. part of the rewritable disc is used as a CD-ROM or DVD-ROM medium. Another implementation is the BCA (Burst Cut Area), a barcode

pattern at the very inner radius of the disc, written by a YAG laser in the disc-factory. A third implementation is to store the fixed data in the radial displacement of the prepressed pits ("pit-wobble") or the radial displacement of the pre-groove ("pre-groove wobble").

Data stored in the recordable data area 3, 4 can be modified by a consumer. Nevertheless, the system data area is reserved for system data like copy protection information as outlined at the beginning. The largest part 4 of the recordable data area can be used for a storing user data, e.g. audio or video data.

Since the capacity of the fixed data 2 area is limited, but a growing amount of system data shall be stored but shall not be modifiable, the invention proposes to store the system data in the recordable data area 3 and to install a cryptographic relationship between the system data and a specific information stored in the fixed data area 2 which can not be modified during subsequent recording or replay. Therefore a cryptographic summary of the system data is computed by the genera-ting means 5, which compute a hash of the system data in this embodiment. The cryptographically secure result of that hash is then stored in the fixed data area 2.

The method described in Fig. 1 is preferably implemented on a recording apparatus for storing the system data and the cryptographic summary on an empty medium using the same or separate recording means.

In the playback apparatus as shown in figure 2 a hash of the system data stored in the system data area 3 is computed by similar generating means 5 contained in the playback apparatus. The result of that computation is forwarded to verifying means 6 in the playback apparatus which also receive the cryptographic summary read from the fixed data area 2 of the medium 1. If this cryptographic summary equals the result of the hash computation the verification is successfull and the playback of user data can start or continue whereas after a verification failure the playback can be stopped since the probabilty is high that the system data have been manipulated. Reading means for reading the system data and the cryptographic summary from the medium are not shown.

In a pratical realization the medium 1 can be imagined as an (at first empty) DVD-RAM or a CD-RW or some other rewritable medium which is sold and contains a list of serial-numbers of known pirated recorders, hereafter referred to as 'naughty' recorders already, written in the disc factory. The list is used by honest players of DVD-RAM/CD-RW ~~or the other media to refuse to playback recordings of these naughty recorders, because they~~ have been known to be involved in illegal copying. Such a list is usually too long (typically more than one MB) to store in a fixed data area (typically a few hundreds of bits). Therefore

the list is written like a normal file on the rewritable medium in the factory. To prevent that anybody just erases or modifies this list, the hash of this list is computed. This hash is much shorter than the system data and can therefore easily be written into the fixed data area during the production of the medium. The honest player then would first, upon insertion of the medium, compute the hash of the system data and check the result with the hash stored in the fixed data area. If they don't match, the system data has been tampered with.

In this basic form no cryptographic secret (e.g. a cryptographic key) has to be used anywhere in the system. A disadvantage is, however, the lack of flexibility. This means that the actual bit-content of the fixed data area on the rewritable medium is fixed forever at the time of the production of the disc in the factory. Thus, the hash has to be computed of the system data that shall be protected prior to production of the disc. If the system data shall be changed, e.g. by adding more naughty recorders to the list, the hash necessarily also changes. New media then have to be produced by the factory, because the old ones no longer have the correct hash for the new system data. There are also other reasons why the system data shall be changed or updated at a time after the production of the disc and fixing of the hash.

More flexibility is achieved in a second embodiment of the invention as shown in figures 3 and 4. According to this embodiment identification data, e.g. a random number, is stored in the fixed data area during production of the medium. The system data area is subdivided into a first area 31 for the actual system data and a second area 32 for storing a cryptographic summary. This cryptographic summary is generated by using a public key signature algorithm computed in the generating means 7. Therein a digital signature of the identification data and the system data which are at first hash-coded by the generating means 5 is computed using a secret private key $K_{private}$. This computation can also be written as

ED = E (hash (system data, identification data), private key)

wherein ED means extra data (=cryptographic summary) and E means the public-key encryption. The computed digital signature is then stored as cryptographic summary in the second system data area 32.

In a replay apparatus or a recording apparatus as shown in figure 4 the system data are verified by at first computing the hash over the identification data and the system data and then using the public key signature verification algorithm in verifying means 8 and the public key K_{public} to check the validity of the signature stored in the data area 32. The private key used for producing the digital signature in figure 3 must be kept secret, while the public key used for verification in the playback or the recording apparatus as shown in figure

4 can be distributed freely, because this public key is useless in the encryption step as described in figure 3.

A third embodiment is explained with reference to figures 5 and 6. As in the second embodiment identification data are stored in a fixed data area 2 and the actual system data are stored in a system data area 31. For encryption the cryptographic summary which shall be stored in the system data area 32 is generated by the generating means 9 from the identification data and the system data using a message authentication code algorithm (MAC algorithm) and a secret MAC key. This MAC-encryption can be in short written as

ED = E (system data, fixed data, MAC-key)

wherein ED means extra data (=cryptographic summary) and E means MAC-encryption.

In the recording or playback apparatus as shown in figure 6 corresponding generating means 9 are provided for computing the message authentication code from the identification data and the system data using the same secret MAC-key. The computed MAC is compared in a verifying means 6 with the cryptographic summary (the MAC) stored in the system data area 32 for verification reasons.

Compared to the second embodiment shown in figures 3 and 4 the use of the MAC is less secure than the use of the public-key signature. The key used to compute the MAC is present in every playback apparatus in the system, if someone breaks open any single player and gets hold of the key, this person can go ahead and replace the system data by other system data that still certify the MAC in the fixed data area. In contrast, in the public-key system of the second embodiment a secret private key is used in the encryption process whereas a published public key is used for verification.

By use of the invention it can be prevented that system data are manipulated. By storing special data in the fixed data area malevolent recorders can be prevented from copying old valid system data to new media, e.g. to replace a new large list of naughty recorders by an old short one. Since the system data itself are stored in the recordable data area the problem of limited capacity of the fixed data area is overcome.

Typically system data is stored or hidden in an area that is inaccessible to the user, or an area of the medium, where it doesn't interfere with the usual purpose of the disc, i. e. with user data storage. For DVD and CD media an example would be the so-called 'lead-in' and 'lead-out' areas of the disc. Hereafter such areas will collectively be referred to as 'corner area'. This has the advantage that it doesn't bother the user, and it also generally makes the production process much cheaper since corner areas can be stamped very fast, whereas recordable data have to be recorded at normal speed. In general players are much cheaper and

simpler than recorders, so it is a relatively larger burden to players than to recorders to read out the system data in the corner area of the medium. So it makes sense to have the recorder, upon first use of the medium, read out the system data and copy its information to the main user data area in the recordable data area. The player can then just find the system data information in the main user data area which it can read anyway. A problem is that the player can not trust the recorder since the latter might not faithfully copy the system data. If, however, as according to the first embodiment of the invention a hash of the system data is stored in the fixed data area, the player can then verify that the incarnation of the system data in the main user data area agrees with the hash in the fixed data area. The recorder obviously can then not have manipulated the fixed data area.

It shall be noted that everytime any detail of the invention is described with reference to a playback apparatus the playback apparatus can be substituted by a recording apparatus. Both may comprise appropriate reading and/or recording means for reading and/or recording of data from or to the medium. Further, it shall be understood that the storage medium, the recording apparatus and the playback apparatus as set forth in the claims can be developed further in the same or a corresponding way as described above and as set forth in the subclaims with reference to the method of storing data.

CLAIMS:

1. Method of storing data on a rewritable data storage medium comprising a read-only fixed data area and a recordable data area wherein:
- system data are stored in the recordable data area,
- a cryptographic summary of the system data is generated and stored in the fixed data area and
- the cryptographic summary is used for verification of the system data before reading and/or recording of user data.

2. Method of storing data on a rewritable data storage medium comprising a read-only fixed data area and a recordable data area wherein:
- system data are stored in the recordable data area,
- identification data are stored in the fixed data area,
- a cryptographic summary of the system data and the identification data is generated and stored in the recordable data area and
- the cryptographic summary is used for verification of the system data before reading and/or recording of user data.

3. Method as set forth in claim 1 or 2, characterized in that a hash function is used for generating the cryptographic summary and for verifying the system data.

4. Method as set forth in claim 1 or 2, characterized in that a message authentication code algorithm is used for generating the cryptographic summary and for verifying the system data.

5. Method as set forth in claim 1 or 2, characterized in that a key signature algorithm is used for generating the cryptographic summary and for verifying the system data and that a signature is stored as cryptographic summary.

6. Method as set forth in claim 1 or 2, characterized in that the cryptographic summary is generated and the system data are stored in the recordable data area as part of the formatting of the storage medium.

7. Method as set forth in claim 1 or 2, characterized in that copy protection information is stored as system data, in particular a unique storage medium identifier, a key encrypted by one or more different manufacturer-specific or device-specific keys or one or more lists of revoked devices or revoked storage mediums.

8. Method as set forth in claim 1 or 2, characterized in that the system data is originally stored in a corner area of the recordable data area and that during first use of the storage medium in a recording apparatus the system data are copied to a user data area of the recordable data area.

9. Storage medium for storing data comprising
- a recordable data area in which system data are stored,
- a read-only fixed data area in which a cryptographic summary of the system data is stored, the cryptographic summary being provided for verification of the system data before reading and/or recording of user data.

10. Storage medium for storing data comprising
- a read-only fixed data area in which identification data are stored,
- a recordable data area in which system data and a cryptographic summary of the system data and the identification data are stored, the cryptographic summary being provided for verification of the system data before reading and/or recording of user data.

11. Storage medium as set forth in claim 9 or 10, characterized in that the storage medium is a rewritable optical storage medium, in particular a CD or a DVD.

12. Recording apparatus for storing data on a rewritable data storage medium comprising
- generating means for generating a cryptographic summary of system data and
- recording means for storing the system data in a recordable data area of the medium and for storing the cryptographic summary in a read-only fixed data area of the medium, the

cryptographic summary being provided for verification of the system data before reading and/or recording of user data.

13. Recording apparatus for storing data on a rewritable data storage medium comprising

- generating means for generating identification data and a cryptographic summary of system data and the identification data and
- recording means for storing the cryptographic summary and the system data in a recordable data area of the medium and for storing the identification data in a read-only fixed data area of the medium, the cryptographic summary being provided for verification of the system data before reading and/or recording of user data.

14. Playback apparatus for playback of user data stored on a rewritable data storage medium comprising

- reading means for reading system data stored in the recordable data area of the medium and for reading a cryptographic summary of the system data stored in a read-only fixed data area of the medium and
- verifying means for generating a cryptographic summary of the system data read from the medium and for verification of the system data by use of the generated cryptographic summary.

15. Playback apparatus for playback of user data stored on a rewritable data storage medium comprising

- reading means for reading identification data from a read-only fixed data area of the medium and for reading system data and a cryptographic summary of the system data and the identification data from a recordable data area of the medium and
- verifying means for generating a cryptographic summary of the system data and the identification data read from the medium and for verification of the system data by use of the generated cryptographic summary.

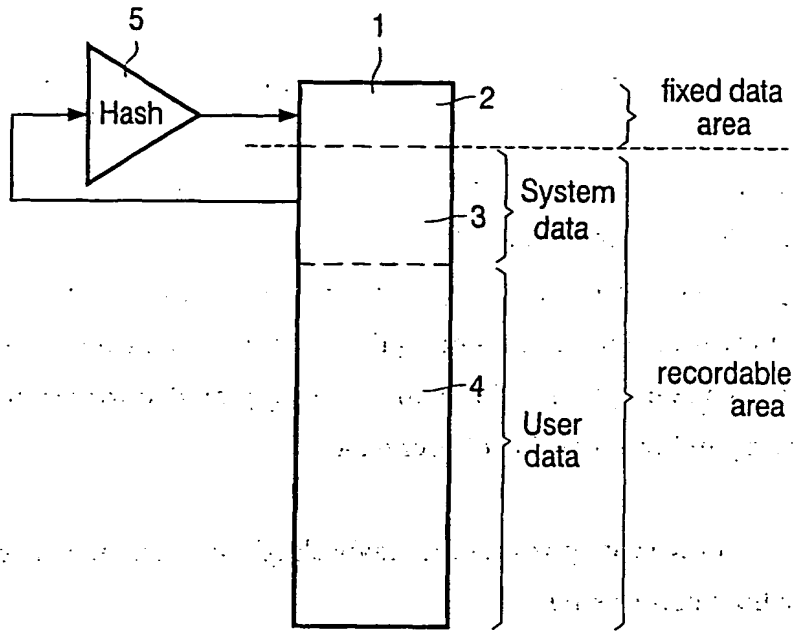

5
1
Hash
2
fixed data area
System data
3
4
User data
recordable data area

FIG. 1

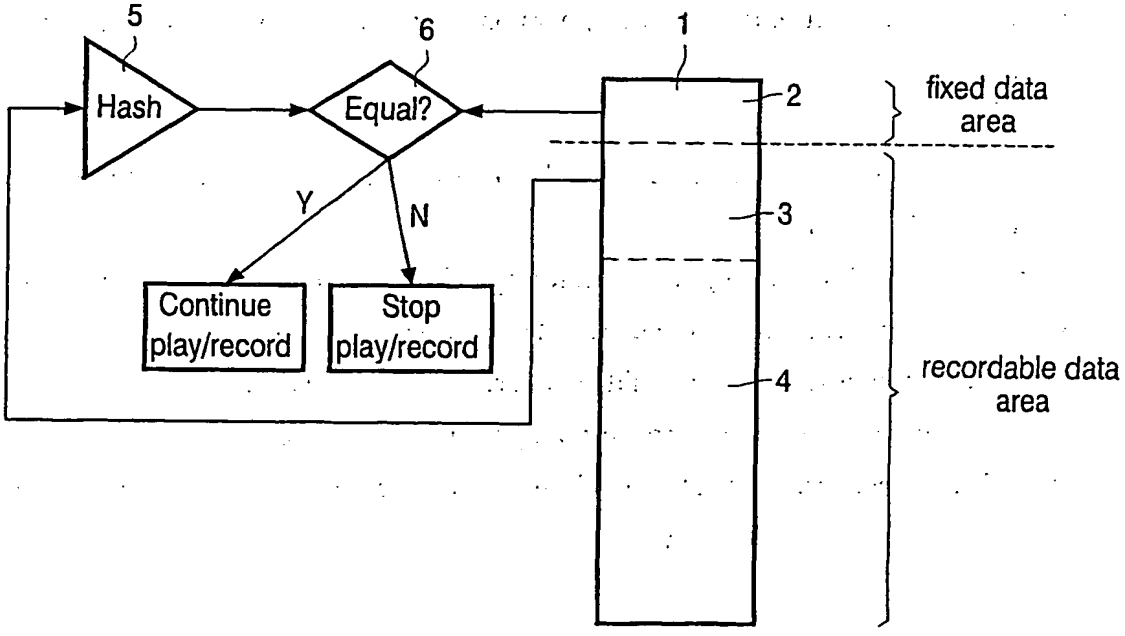

5
6
1
Hash
Equal?
2
fixed data area
Y
N
3
Continue play/record
Stop play/record
4
recordable data area

FIG. 2

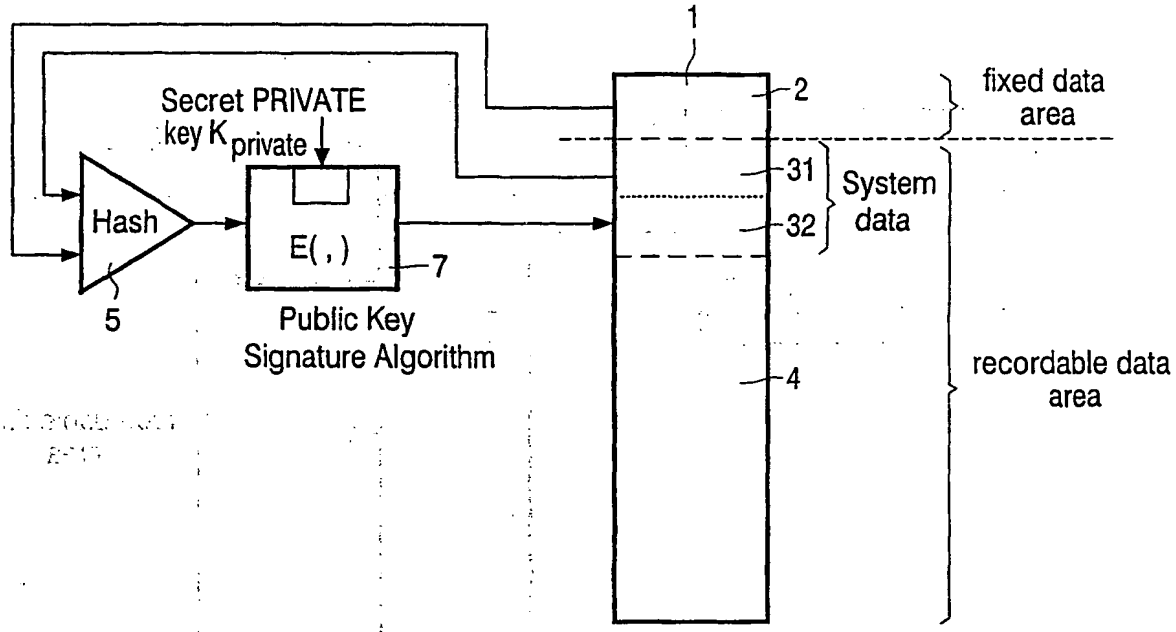

1
2
fixed data area
Secret PRIVATE key K private
31
System data
32
Hash
E(,)
7
5
Public Key Signature Algorithm
4
recordable data area

FIG. 3

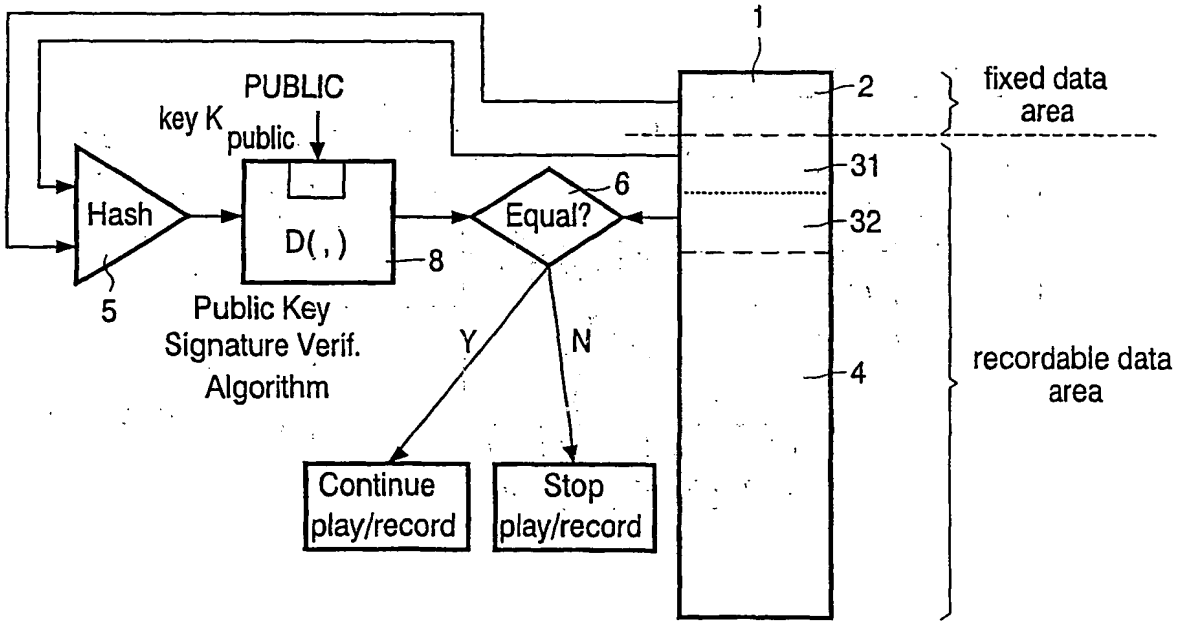

1
2
fixed data area
PUBLIC key K public
31
6
Hash
Equal?
32
D(,)
8
5
Public Key Signature Verif. Algorithm
Y
N
4
recordable data area
Continue play/record
Stop play/record

FIG. 4

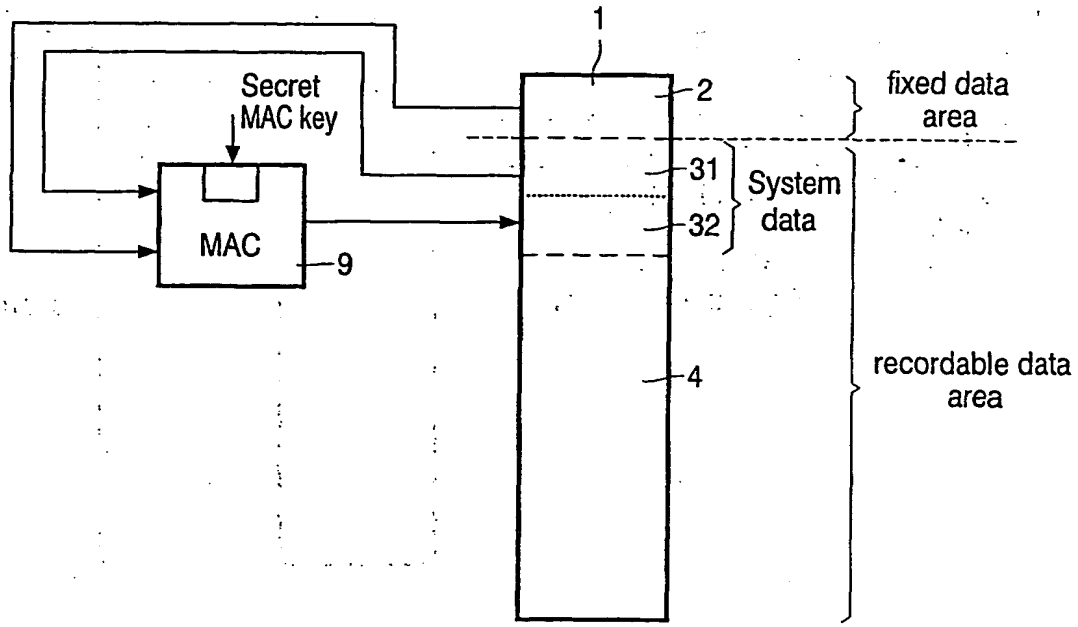

1
Secret
MAC key
MAC
9
2
fixed data
area
31
32
System
data
4
recordable data
area

FIG. 5

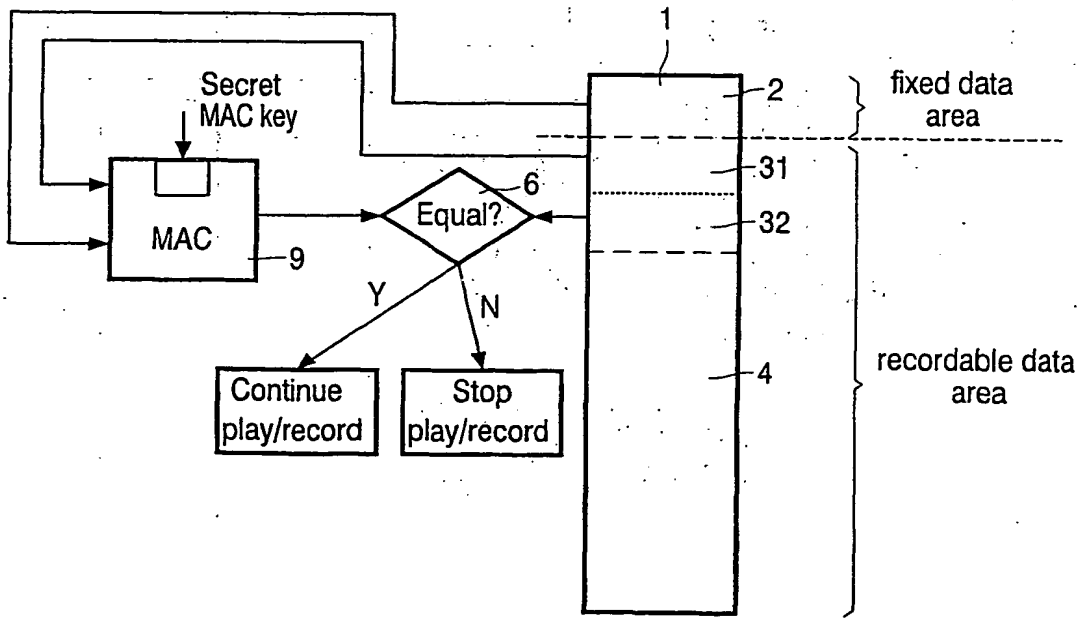

1
Secret
MAC key
MAC
9
Equal?
6
Y
N
Continue
play/record
Stop
play/record
2
fixed data
area
31
32
4
recordable data
area

FIG. 6

THIS PAGE BLANK (USPTO)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 December 2001 (13.12.2001)

PCT

(10) International Publication Number
WO 01/95327 A3

(51) International Patent Classification[7]: G11B 20/00, 20/12

(21) International Application Number: PCT/EP01/05195

(22) International Filing Date: 8 May 2001 (08.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
00201951.1 2 June 2000 (02.06.2000) EP

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors: LINNARTZ, Johan, P., M., G.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). KALKER, Antonius, A., C., M.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). TALSTRA, Johan, C.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: DEGUELLE, Wilhelmus, H., G.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

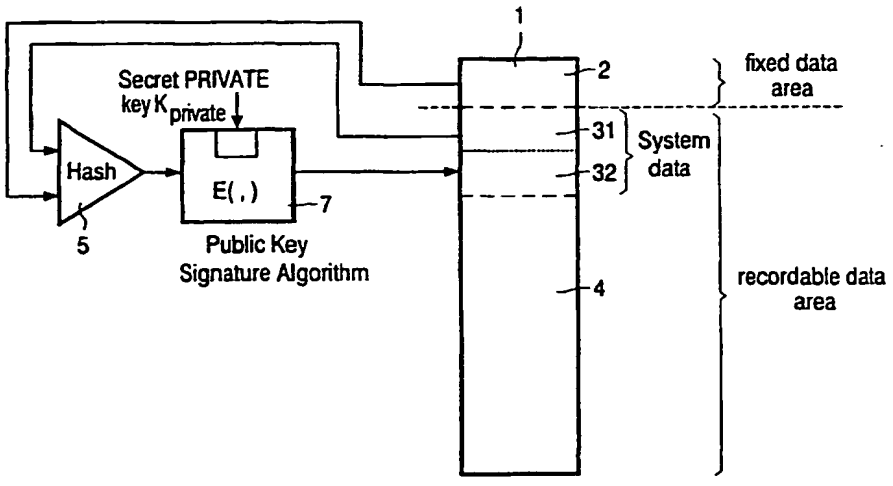
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: RECORDABLE STORAGE MEDIUM WITH PROTECTED DATA AREA



(57) Abstract: The invention relates to a method of storing data on a rewritable data storage medium, to a corresponding storage medium, to a corresponding recording apparatus and to a corresponding playback apparatus. Copy-protective measures require that on rewritable storage media some data must be stored which shall not be modifiable or erasable by consumer end products. A practical problem is the storage of large quantities of such data in a fixed data area. Typically the capacity is limited to a few bits. Meanwhile the amount of copy protection data that needs to be stored may well exceed the storage capacity available in the read-only fixed data area. The invention therefore proposes to write the copy protection data as system data in the recordable data area (4), e.g. as part of the formatting of the medium (1). A cryptographic summary is computed and also stored in the recordable data area (32) or in the fixed data area (2) such that a cryptographic relationship between the fixed data area (2) and the system data area (3) is provided. A playback or replay apparatus will only accept a storage medium with a valid combination of copy protection data and fixed data.

WO 01/95327 A3

(88) Date of publication of the international search report:
21 March 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

Inte. .onal Application No
PCT/EP 01/05195

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 G11B20/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	EP 0 984 346 A (HITACHI EUROP LTD) 8 March 2000 (2000-03-08) column 4, line 22 -column 7, line 47 column 9, line 42 -column 10, line 11 column 15, line 17 - line 20 ---	2-5,10, 11,13,15 1,9,12, 14
A	EP 0 997 899 A (MATSUSHITA ELECTRIC IND CO LTD) 3 May 2000 (2000-05-03) column 5, line 53 -column 8, line 12 column 25, line 49 -column 26, line 27; claims 1,2,6,7 ---	1,2,9-15
A	US 5 761 301 A (GOTOH YOSHIHO ET AL) 2 June 1998 (1998-06-02) column 26, line 38 - line 42 column 30, line 54 - line 58 --- -/--	1,2,9-15

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 December 2001	12/12/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Brunet, L

2

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 982 886 A (NARUMI TOSHIKATSU ET AL) 9 November 1999 (1999-11-09) column 9, line 43 - line 52 column 13, line 1 -column 14, line 8 ---	1,2,9-15
A	US 6 028 936 A (HILLIS W DANIEL) 22 February 2000 (2000-02-22) column 2, line 51 -column 3, line 34 column 4, line 14 -column 5, line 13 ---	1,2,9-15
A	EP 0 593 305 A (MATSUSHITA ELECTRIC IND CO LTD) 20 April 1994 (1994-04-20) column 3, line 17 -column 4, line 48 ---	1,2,9-15
A	US 5 752 009 A (NAKAHARA MASARU ET AL) 12 May 1998 (1998-05-12) column 9, line 51 -column 10, line 31 column 15, line 1 - line 26 column 22, line 51 - line 57 -----	1,2,9-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte. ional Application No
PCT/EP 01/05195

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0984346 A	08-03-2000	EP 0984346 A1	08-03-2000
		JP 2000076141 A	14-03-2000
EP 0997899 A	03-05-2000	CN 1248766 A	29-03-2000
		EP 0997899 A2	03-05-2000
		JP 2000163883 A	16-06-2000
US 5761301 A	02-06-1998	CN 1127049 A	17-07-1996
		CN 1138915 A	25-12-1996
		DE 69523139 D1	15-11-2001
		EP 1120777 A2	01-08-2001
		EP 0706174 A1	10-04-1996
		EP 0741382 A1	06-11-1996
		JP 8273164 A	18-10-1996
		WO 9528704 A1	26-10-1995
		WO 9616401 A1	30-05-1996
		US 5881038 A	09-03-1999
		US 5805551 A	08-09-1998
		CN 1166223 A	26-11-1997
		CN 1173942 A	18-02-1998
		DE 69610859 D1	07-12-2000
		DE 69610859 T2	15-03-2001
		DE 69610860 D1	07-12-2000
		DE 69610860 T2	15-03-2001
		DE 69610861 D1	07-12-2000
		DE 69610861 T2	15-03-2001
		DE 69611906 D1	05-04-2001
		DE 69611906 T2	21-06-2001
		DE 69613010 D1	28-06-2001
		DE 69613010 T2	15-11-2001
		DE 69613011 D1	28-06-2001
		DE 69613011 T2	15-11-2001
		DE 69613156 D1	05-07-2001
		DE 69613156 T2	25-10-2001
		DE 69614580 D1	20-09-2001
		DE 69614823 D1	04-10-2001
		DE 69615418 D1	25-10-2001
		EP 1005033 A1	31-05-2000
		EP 1005034 A1	31-05-2000
		EP 1005023 A1	31-05-2000
		EP 1005024 A1	31-05-2000
		EP 1005025 A1	31-05-2000
		EP 1005026 A1	31-05-2000
		EP 1005027 A1	31-05-2000
		EP 1024478 A1	02-08-2000
		EP 1005028 A1	31-05-2000
		EP 1003162 A1	24-05-2000
		EP 1005035 A1	31-05-2000
		EP 1006516 A1	07-06-2000
		EP 1006517 A1	07-06-2000
		EP 1028422 A1	16-08-2000
		EP 1028423 A1	16-08-2000
		EP 1030297 A1	23-08-2000
		EP 1031974 A1	30-08-2000
		EP 0807929 A1	19-11-1997
		EP 0802527 A1	22-10-1997
US 5982886 A	09-11-1999	JP 2575987 B2	29-01-1997

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte. ional Application No
PCT/EP 01/05195

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5982886 A		JP 5266574 A	15-10-1993
		JP 2575988 B2	29-01-1997
		JP 5266575 A	15-10-1993
		JP 2575989 B2	29-01-1997
		JP 5266576 A	15-10-1993
		JP 2582507 B2	19-02-1997
		JP 5325418 A	10-12-1993
		DE 4308680 A1	28-10-1993
		US 5418852 A	23-05-1995
US 6028936 A	22-02-2000	NONE	
EP 0593305 A	20-04-1994	JP 3084969 B2	04-09-2000
		JP 6131806 A	13-05-1994
		EP 1132908 A2	12-09-2001
		EP 1132911 A2	12-09-2001
		EP 0593305 A2	20-04-1994
		EP 0803872 A2	29-10-1997
		US 5974140 A	26-10-1999
US 5752009 A	12-05-1998	EP 1076331 A2	14-02-2001
		EP 0634741 A1	18-01-1995
		JP 2891877 B2	17-05-1999
		JP 7078187 A	20-03-1995
		KR 186891 B1	15-04-1999